DOCKET 207312

PATENTS • DESIGNS • COPYRIGHT • TRADE MARKS
The Patent Office

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

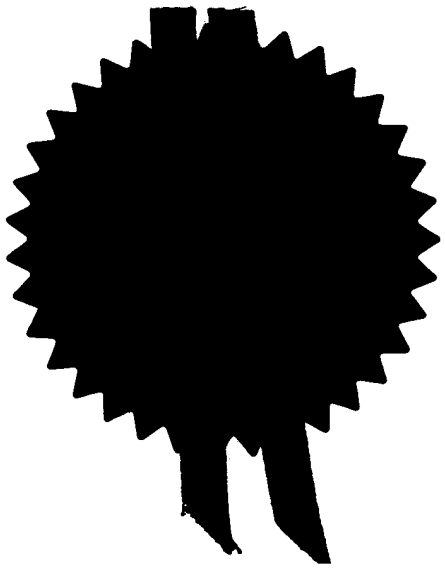
CERTIFIED COPY OF
PRIORITY DOCUMENT

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.



Signed

Dated: 14 November 2000

Patents Form 1/77

Patents Act 1977
(Rule 16)

THE PATENT OFFICE
D
18 NOV 1999
LONDON

The Patent Office

19NOV99 E493053-1 D02855
P01/7700 0.00-9927334.4

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
Gwent NP9 1RH

1. Your reference — 18/P32379GB — 18 NOV 1999

2. Patent application number
(The Patent Office will fill in this part) — 9927334.4

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

VODAFONE LIMITED

The Courtyard
2-4 London Road
Newbury, Berkshire, RG14 1JX, U.K.

Patents ADP number *(if you know it)*

If the applicant is a corporate body, give the country/state of its incorporation — U.K. 6227912002

4. Title of the invention

USER AUTHENTICATION IN A MOBILE COMMUNICATIONS NETWORK

5. Name of your agent *(if you have one)*

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

Mathisen, Macara & Co

The Coach House
6-8 Swakeleys Road, Ickenham
Uxbridge, UB10 8BZ, U.K.

Patents ADP number *(if you know it)* — 1073001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

Yes

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	8
Claim(s)	5
Abstract	1
Drawing(s)	1

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	
Request for preliminary examination and search *(Patents Form 9/77)*	1
Request for substantive examination *(Patents Form 10/77)*	
Any other documents *(please specify)*	

11. I/We request the grant of a patent on the basis of this application.

Signature [signature] Date 18 November 1999

Mathisen, Macara & Co

12. Name and daytime telephone number of person to contact in the United Kingdom ANDREW B MACKENZIE +44(0)1895 678331

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.

b) Write your answers in capital letters using black ink or you may type them.

c) If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.

d) If you have answered 'Yes' Patents Form 7/77 will need to be filed.

e) Once you have filled in the form you must remember to sign and date it.

f) For details of the fee and ways to pay please contact the Patent Office.

DUPLICATE

UNITED KINGDOM PATENT APPLICATION

APPLICANTS: VODAFONE LIMITED

SHORT TITLE: "Single Vector"

FORMAL TITLE: USER AUTHENTICATION IN A MOBILE COMMUNICATIONS NETWORK

APPLICATION NO:

FILED:

PRIORITY CLAIMED: NIL

MATHISEN, MACARA & CO.
6 - 8 Swakeleys Road,
Ickenham, Uxbridge,
England, UB10 8BZ

Agents for the Applicants

USER AUTHENTICATION IN A MOBILE COMMUNICATIONS NETWORK

This invention relates to a method and apparatus for authenticating mobile user equipment in a mobile telecommunications network.

In accordance with a first aspect of the invention, there is provided a method of authenticating mobile user equipment in a mobile telecommunications network comprising the steps of passing an authentication element forming at least part of an authentication vector, from a serving network to mobile user equipment, deciding in the user equipment based at least in part on the value of a predetermined field contained in the authentication element, when to generate a termination message, and passing the termination message from the mobile user equipment to the serving network which message contains a value indicating that the serving network must obtain a further authentication vector before allowing the user equipment to make further calls.

In accordance with a second aspect of the invention, there is provided a method of authenticating mobile user equipment in a mobile telecommunications network comprising the steps of requesting service from a serving network to which the user equipment is not directly subscribed, passing the request for service from the serving network to a home operator network to which the user equipment is directly subscribed, generating an authentication vector in the home operator network which includes an authentication management field, passing the authentication vector from the home operator network to the

serving network, passing an authentication element forming at least part of the authentication vector from the serving network to the user equipment, extracting in the user equipment an authentication management field from the authentication element, generating in response at least to a predetermined value of the authentication management field, a predetermined key set identifier, and passing the key set identifier to the serving network.

In accordance with a third aspect of the invention, there is provided mobile user equipment for use in a mobile telecommunications network including means for receiving from a serving network, an authentication element forming at least part of an authentication vector, decision means for deciding in the user equipment based at least in part on the value of a predetermined field contained in the authentication element, when to generate a termination message, and means for passing the termination message from the mobile user equipment to the serving network which message contains a value indicating that the serving network must obtain a further authentication vector before allowing the user equipment to make further calls.

Embodiments of networks and mobile user equipment in accordance with the invention will now be described by way of example with reference to the drawings in which:

Figure 1 is a schematic diagram of the flow of authentication information between a serving network and a home environment;

Figure 2 is a schematic block diagram of the processing of an authentication vector by mobile user equipment; and

Figure 3 is a schematic block diagram showing the flow of key set identification information between a mobile user and the visitor location register of a serving network.

The invention described below permits a 3GPP operator to use the 3GPP authentication management field AMF to direct a subscriber of that operator to ensure that a particular 3GPP authentication vector for that subscriber (from that operator) is used for only one call in a particular serving network. Alternatively the authentication vector may be used only for a predetermined time period, for a predetermined number of calls or for a predetermined total call duration (which may span more than one call) after issuance by the operator or receipt by the user equipment. The invention is applicable, for example, to 3GPP, 3GPP2, and IS-136 networks and to ANSI-41 networks which adopt the TR45 Enhanced Subscriber Authentication (ESA).

One possibility which has been considered is for a serving network (i.e. the network that a user is making calls with) to be given instructions on how the authentication vector should be used. However, this would require the home operator or home environment (i.e. the operator with which the user has a subscription) to rely on the competence of the serving network to ensure that the instructions are correctly followed. Furthermore, assuming that the instructions are passed electronically, new signalling messages would

need to be standardised and new procedures in the serving network visitor location registers (VLR's) would need to be devised, standardised and implemented to ensure that the VLR's respond correctly to the new signalling messages.

With reference to Figure 1, an authentication vector is transmitted from the home operator HE to the serving network SN in response to a so called "authentication data request" from the serving network.

An authentication vector contains the following parameters

RAND which is a random challenge generated by the home operator,

XRES which is the expected user response to RAND which is pre-computed by the home operator,

CK which is a cipher key,

IK which is an integrity key, and

a network user authentication string AUTN.

The network to user authentication string AUTN consists of

the sequence number for the vector (SQN) which is concealed with an anonymity key (AK),

an authentication management field AMF (discussed in detail below), and

a message authentication code MAC-A which allows for network to user authentication.

Having received an authentication vector from the home environment, the serving network passes the RAND and AUTN portions of the vector to the user equipment.

With reference to Figure 2, the RAND and AUTN portions are processed by the mobile user equipment. The user equipment processes RAND using a predetermined algorithm f5 which takes as its input also a long term secret key K. This produces the anonymity key AK which can be used to reveal the sequence number SQN.

SQN is then fed into a predetermined algorithm f1 along with RAND and the long term secret key K. This generates XMAC (the expected message authentication code). This is compared with MAC-A and should be equal to MAC-A.

If XMAC is correct, the user equipment then checks that the sequence number SQN which has been generated is greater than SQN_{he}; which is the SQN attached to the last valid

RAND/AUTN combination received from the home environment. This ensures that an authentication vector can only be used once.

If both MAC-A and SQN in the network to user authentication string AUTN pass the above test, then the AUTN is considered valid. The user equipment then processes RAND by applying the long term secret key K via algorithms f2, f3 and f4. This generates the values of RES, IK and CK.

The response (RES) is sent to the serving network which responds with a key set identifier (KSI). The user SIM assigns or tags the generated CK and IK values with the KSI given by the serving network. As described below, the user equipment then passes the KSI to the SN with each request for service.

As noted above, it may be difficult for the home operator to ensure that correct authentication procedures are carried out by the serving network. Described below, are several techniques (which may be selected by sending appropriate instructions via the authentication management field of the authentication vector) which limit the lifetime of the authentication vector thereby requiring the serving network to request a new authentication vector from the home operator.

With reference to Figure 3, once the process shown in Figure 2 is completed, the user equipment may initiate calls via the serving network using the same KSI without requiring

a new vector to be requested by the serving network. Initially, the user equipment sends its current KSI in its first layer three message (this being the message that requests a particular service from the serving network). The serving network checks the KSI received with the message and if it is valid, continues to process the service request. Ciphering and integrity protection are performed using the CK and IK indicated by the KSI.

The user equipment is able to select a KSI value which indicates to the serving network that the user does not have a valid CK or IK at the next service request (for example the next call). Thus, without modifying any of the signalling messages between the home operator and serving network or producing any new procedures for the serving network VLR, it is possible for the user equipment to control the lifetime of the authentication vector.

In the first technique, the authentication management field is used to instruct the user equipment to always issue a KSI which causes a new vector to be requested when service is next requested from the serving network. The effect of this is that an authentication vector is requested for every call made by the user equipment in the serving network. This ensures that full authentication occurs for every call and also means that the home operator is notified of every call made by the user equipment. This means that the home operator has control over the security of the use of the user equipment in the serving network.

In an alternative approach, the user equipment can allow the authentication vector to be used for a predetermined time period, a predetermined number of calls or a predetermined

total call duration (which may span more than one call). These parameters may be monitored by the user equipment using appropriate timers, accumulators and counters. Before requesting service, the mobile user equipment determines whether the authentication vector should still be valid and issues either the KSI given by the serving network (if no new authentication vector is required) or a special KSI which forces the serving network to request a new authentication vector when the next service request is made.

Thus in the first technique above, the AMF may be used to ensure that only one call can be made with the authentication vector containing that AMF. This provides maximum security for the home operator. In the alternative techniques, the risk to the home operator of abuse of the network is reduced because there is choice of a maximum time limit of service, maximum call duration and/or maximum number of calls available with a particular authentication vector.

It will be appreciated that the user equipment may be arranged to implement one, all or a selection of the above techniques, each selected by a particular value of the AMF. Also, the user equipment may implement a combination of the techniques such as forcing a new vector to be requested if a predetermined number of calls have been made or a predetermined time period has expired.

CLAIMS

1. A method of authenticating mobile user equipment in a mobile telecommunications network comprising the steps of:

passing an authentication element forming at least part of an authentication vector, from a serving network to mobile user equipment,

deciding in the user equipment based at least in part on the value of a predetermined field contained in the authentication element, when to generate a termination message, and

passing the termination message from the mobile user equipment to the serving network which message contains a value indicating that the serving network must obtain a further authentication vector before allowing the user equipment to make further calls.

2. A method according to claim 1, wherein the termination message is a predetermined key set identity value.

3. A method according to claim 1 or claim 2, wherein the predetermined field is an authentication management field.

4. A method according to any preceding claim, wherein the said decision is taken based on the total call duration which has accumulated since the authentication

element containing the predetermined field was first received by the mobile user equipment.

5. A method according to any preceding claim, wherein the said decision is taken based on the time elapsed since the authentication element containing the predetermined field was first received by the mobile user equipment.

6. A method according to any preceding claim, wherein the said decision is taken based on the total number of calls made since the authentication element containing the predetermined field was first received by the mobile user equipment.

7. A SIM for mobile user equipment embodying the method steps of any preceding claim.

8. A method of authenticating mobile user equipment in a mobile telecommunications network comprising the steps of:

requesting service from a serving network to which the user equipment is not directly subscribed,

passing the request for service from the serving network to a home operator network to which the user equipment is directly subscribed,

generating an authentication vector in the home operator network which includes an authentication management field,

passing the authentication vector from the home operator network to the serving network,

passing an authentication element forming at least part of the authentication vector from the serving network to the user equipment,

extracting in the user equipment an authentication management field from the authentication element,

generating in response at least to a predetermined value of the authentication management field, a predetermined key set identifier, and

passing the key set identifier to the serving network.

9. A method according to claim 8, including deciding in the user equipment based at least in part on the value of a predetermined field contained in the authentication element, when to generate a key set identifier which contains a value indicating that the serving network must obtain a further authentication vector before allowing the user equipment to make further calls.

10. A method according to claim 9, wherein the said decision is taken based on the total call duration which has accumulated since the authentication element containing the predetermined field was first received by the mobile user equipment.

11. A method according to claim 9 or claim 10, wherein the said decision is taken based on the time elapsed since the authentication element containing the predetermined field was first received by the mobile user equipment.

12. A method according to any one of claims 9 to 11, wherein the said decision is taken based on the total number of calls made since the authentication element containing the predetermined field was first received by the mobile user equipment.

13. Mobile user equipment for use in a mobile telecommunications network including means for receiving from a serving network, an authentication element forming at least part of an authentication vector, decision means for deciding in the user equipment based at least in part on the value of a predetermined field contained in the authentication element, when to generate a termination message, and means for passing the termination message from the mobile user equipment to the serving network which message contains a value indicating that the serving network must obtain a further authentication vector before allowing the user equipment to make further calls.

14. Mobile user equipment according to claim 13, including accumulator means for monitoring the total call duration which has accumulated since the authentication element containing the predetermined field was first received by the mobile user

equipment and providing a value representative of the said total call duration to the decision means.

15. Mobile user equipment according to claim 13 or claim 14, including timer means for measuring the time elapsed since the authentication element containing the predetermined field was first received by the mobile user equipment and providing a value representative of the said elapsed time to the decision means.

16. Mobile user equipment according to any one of claims 13 to 15, including counter means for counting the total number of calls made since the authentication element containing the predetermined field was first received by the mobile user equipment and providing a value representative of the said total call number to the decision means.

17. A mobile communications network constructed and arranged as described herein with reference to the drawings.

18. Mobile user equipment constructed and arranged as described herein with reference to the drawings.

ABSTRACT (Fig. 2)

A method of authenticating mobile user equipment in a mobile telecommunications network comprising the steps of receiving an authentication element from a serving network (SN) to which the user equipment is not directly subscribed, extracting the authentication management field (AMF) from the authentication element, generating in response at least to a predetermined value of the authentication management field (AMF), a key set identifier (KSI), and passing the key set identifier (KSI) to the serving network (SN).

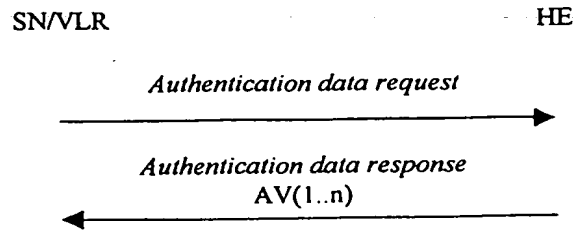


Figure 1

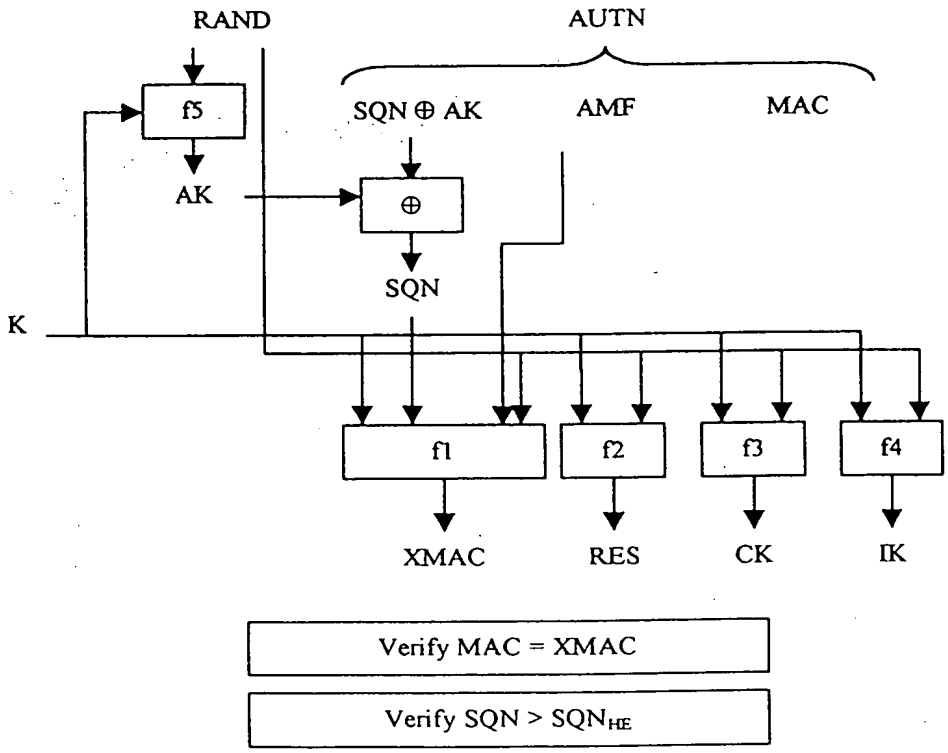


Figure 2

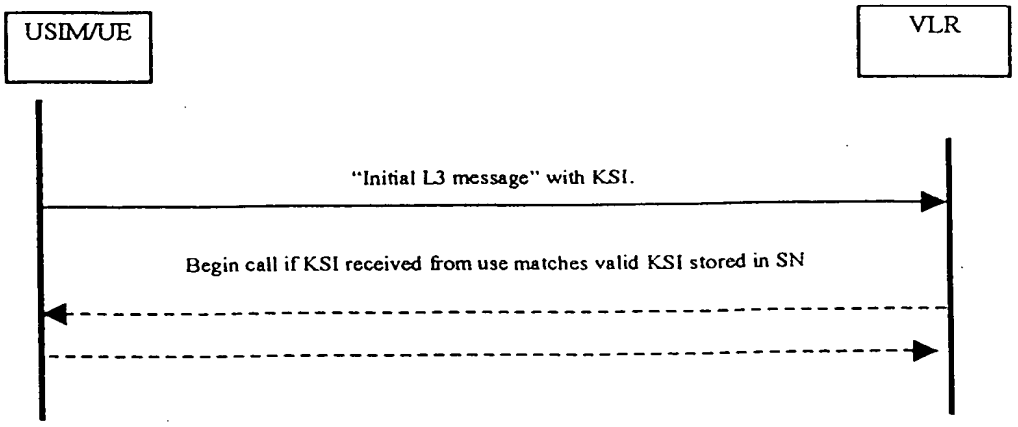


Figure 3